# Mitigations Against Current High Profile Attacks





September 2015

### Introduction

You've read about them, you may even have had to respond to them, major cyber incidents that have shown up in the national and international press. These significant incidents have led to the loss of intellectual property, personally identifiable information, financial information and corporate integrity resulting in embarrassment. While the number of reported cyber attacks has been increasing, far more incidents never make the ticker at the bottom of your TV screen, or the lead story in the news.

The reality is that most of those high profile incidents could have been prevented. They didn't need a silver bullet, what they needed was basic network and computer hygiene and strong cyber security practices. That said, securing your networks can feel overwhelming given the variety of cyber threats, the maze of buzzwords, seemingly convincing product literature and the stacks of security guidance available.

In order to understand how the majority of high profile intrusions occurred, it is important to understand the most common attack vectors that were utilized and the NSA-recommended mitigations designed to prevent them.

# **Recently Observed Attack Vectors**

#### **Spear Phishing**

Spear phishing utilizes embedded malicious links or attachments in targeted e-mails to infiltrate a network. These embedded links can lead to attacks on vulnerable web browsers, allowing the execution of malicious content. Once the malware is executed, the adversary can install command and control capabilities to extract or destroy sensitive information or even destroy a system, like an industrial control system.

#### **Memory Mining**

Memory mining malware inspects vulnerable areas in memory where data passes unencrypted to obtain private keys or other sensitive data. Credential theft tools find passwords, tickets, and other forms of credentials to enable lateral movement to other systems and data. RAM scrapers can steal customer payment information from a Point-of-Sale system while it is unencrypted for processing.

#### **Data Destruction**

Data destruction occurs when adversaries gain unauthorized access to networks and systems to maliciously tamper with or delete information. It is important to secure financial data, trade secrets and personal information on employees and clients for confidentiality, integrity and availability.

#### **Backdoor Attacks**

Backdoors are usually put into a system to allow access for maintenance or if original access is lost. Backdoors can also be inserted through the introduction of malware. This malware creates a backdoor or unauthorized access that allows an attacker to collect computer and network information. The backdoor can be used to install additional attack tools and destructive malware. This malware is often used to gain persistent access to domain controllers, other critical servers, and supervisory control and data acquisition (SCADA) systems.

#### **Lateral Movement**

Once an adversary has penetrated the external boundary of a network they will extend their access inside by moving laterally. This is accomplished through network mapping, scanning the environment for vulnerabilities and though Pass-the-Hash (PtH) attacks; all of which collect new credentials to gain further access.

## **DDoS**

Distributed Denial of Service (DDoS) attacks leverage bandwidth from botnets or high-bandwidth sites to flood victim networks with protocol traffic to disrupt or deny requests from customers. DDoS attacks can slow down the network, disrupt ongoing business and transactions, and make it more difficult for network administrators to clearly see other activities taking place.

# Mitigations Against Current High Profile Attacks





# Way Ahead - Mitigations & Hygiene

So where do you start? The best mitigations to combat these attack vectors are to properly patch, have strong configuration control and implement capabilities that stop malware execution. Networks should be segregated to contain potential damage and elevated privileges should be restricted in order to reduce the risk of adversaries moving laterally throughout the entire network. Additionally, limiting access to sensitive information by implementing network segregation will limit data loss. Lastly, safeguards need to be put in to place to stop DDoS and maintain information confidentiality, integrity, and availability.

Patching and configuration control play a significant role in securing networks against the previously stated attacks and regularly issued guidance validates the need to implement these mitigations. Although they are best practice mitigations, patching and configuration control will not be included here due to the inordinate amount of guidance.

## **Stop Malware Execution**

Application whitelisting can be utilized to prevent executables, including those introduced via adversarial attacks such as spear phishing, from executing. Application Whitelists are created and maintained by administrators to proactively disallow unapproved executables and applications from running and only allow those which are approved by the organization to execute. There are several different types and maturity levels of application whitelisting that have differing costs and security benefits. Path-based whitelisting is fairly low cost and provides a good initial balance between security and usability.

Anti-exploitation features that are available in commercial products provide protection against exploits based on the behaviors of the code that is executing. These products are able to identify exploitation attempts, isolate and stop the execution, log the event and notify the system administrator. Anti-exploitation features are especially effective against common attacks meant for mass infection, such as drive-by download sites and phishing campaigns.

A Host Intrusion Protection System (HIPS) is a centrally managed tool that allows administrators to push policies down to specific hosts. Alerts of malicious activity are then sent up to the administrators to decide what actions should be taken. Products should use signature detection approaches targeting specific known-bad pieces of code or malicious files and behavioral detection methods for unknown code or files.

#### **Data Loss and Destruction**

Data loss prevention controls help stop the loss of data on network, server and workstation devices. Networks should be segregated in order to prevent adversaries from accessing and destroying data in multiple enclaves. Backups of critical systems should reside at an offsite location and should be tested regularly. Incident response plans should include communication procedures, roles and responsibilities, reporting methods and data recovery processes.

# **Preventing Lateral Movement**

Implement a least-privilege administrative model, only granting users those privileges needed to do their jobs, and protect privileged credentials by restricting how and where they can be used. Pass-the-Hash (PtH) is a commonly used technique used to elevate privileges or gain access to sensitive information. Many of the recommendations associated with PtH can assist with restricting forms of adversarial lateral movement and access. Limiting workstation-to-workstation communications will significantly restrict attackers' freedom of movement.

In general, limiting communication flows between systems also aids in the detection of potentially malicious network activity. Properly segregated networks utilize separate infrastructure for each functional area within an organization. This includes providing separate servers, storage devices, routers, and switches for different areas of varying sensitivity and access.

#### **DDoS**

DDoS attacks are difficult to prevent, but there are security mechanisms and network design strategies that can mitigate attacks and minimize their impact. Proactive measures include having multiple Internet connections

MFS U/OO/813937-15

# Mitigations Against Current High Profile Attacks





with prenegotiated capabilities that can automatically deal with bandwidth saturation. Build a perimeter defense that balances traffic load across multiple Internet connections. The perimeter boundary defending your network from DDoS should include premise router access control, an Intrusion Detection System (IDS) and a firewall. Networks should be designed with redundant systems and conduct rate-limiting of traffic at the perimeter.

#### Conclusion

The media only reports one side of the story: the latest intrusion, the loss of vital national data, and the millions of dollars lost. The reality is that network security is achievable. There are strategies, processes, and mitigations that can further assist in staying ahead of the cyber adversary.

For further detailed operational and implementation guidance on the above mitigation topics, please refer to our publication "NSA Methodology for Adversary Obstruction": at https://www.nsa.gov/ia/\_files/factsheets/NSA\_Methodology\_for\_Adversary\_Obstruction.pdf

Please refer to the IA Top 10 Mitigation Strategies here:

https://www.nsa.gov/\_files/factsheets/I43V\_Slick\_Sheets/Slicksheets\_Top10IAMitigationStrategies\_Web\_pdf

For best defensive practices against destructive malware please visit:

https://www.nsa.gov/ia/\_files/factsheets/Defending\_ Against\_Destructive\_Malware.pdf

For a complete list of IA Mitigation Guidance please visit:

https://www.nsa.gov/ia/mitigation\_guidance/index.shtml

# **Disclaimer**

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

## **Contact Information**

### **Industry Inquiries**

410-854-6091 email: bao@nsa.gov

# Client Requirements and General Information Assurance Inquiries

IAD Client Contact Center 410-854-4200 email: IAD\_CCC@nsa.gov